في العالم الذي نعيشه اليوم، تتداخل خيوط التكنولوجيا في كل جانب من جوانب حياتنا، فهي تلمع كنجم لامع في سماء الإنسانية ، تفتح أبواباً للمعرفة والابتكار، ولكنها في الوقت ذاته، تكشف عن وجه آخر ليس بتلك البراءة

مع ازدياد الاعتماد على الشبكات الرقمية، انتقلت الجرائم والاعتداءات من الفضاء المادي إلى الساحة السيبرانية، وفي هذه الأثناء، تبقى الجرائم الإلكترونية غموضاً يحيط بالجميع، ملقيًا بظلاله الكئيبة على الحياة الرقمية

لهذا السبب تم تأليف هذا الكتاب "الأمن السيبراني: رحلة لعالم الجرائم الإلكترونية وطرق التصدي لها من منظور قانوني وتقني" يمثل هذا العمل الرائد عبورًا للمعرفة البشرية، والذي يتناول تفاصيل الهجمات السيبرانية وأنواعها، كما يتطرق إلى سبل الدفاع والتصدي لها بفعالية

في أروقته، يرتقي الكتاب بقارئه لمستوى أعلى من الوعي الأمني، ويسلط الضوء على الآليات القانونية التي تحمي الناس وتحافظ على أمنهم في الفضاء السيبراني. هنا، يجد القارئ نفسه في رحلة مثيرة، بين القانون والتقنية، لاكتشاف الأساليب الذكية للتصدي للتهديدات السيبرانية

هذا الكتاب هو الرفيق المثالي لكل من يرغب في تنقيب أعماق عالم الأمن السيبراني، والقانون، والتكنولوجيا، وسيكون له صدى في ذاكرة كل قارئ يستعرض صفحاته

فهل أنتم مستعدون لتكونوا رواد هذه الرحلة الشيقة؟ هل أنتم مستعدون لكشف النقاب عن وجه الجريمة الإلكترونية ومعرفة كيفية التصدي لها؟ هل أنتم مستعدون للدخول في عالم الأمن السيبراني العجيب؟ أتمنى لكم قراءة ممتعة ومفيدة في هذا الكتاب

محمد عبدالنبي

الجريمة السيبرانية والامن السيبراني

الأمن السيبراني بكل بساطة يعني الحماية التي نقدمها لأجهزتنا الإلكترونية، مثل حماية الكمبيوتر والهاتف المحمول، وحتى حساباتنا الشخصية على الإنترنت ضد أي محاولات للتجسس أو السرقة

على سبيل المثال، عندما تستخدم برنامجًا لمكافحة الفيروسات على جهازك، هذا يعد جزءًا من الأمن السيبراني.أو عندما تغير كلمة السر الخاصة بك بشكل دوري، هذا أيضًا يعتبر جزءًا من الأمن السيبراني.

أما الجريمة السيبرانية، فهي مثل الجرائم التقليدية ولكن في العالم الرقمي. هذا يشمل الأمور مثلا عندما يحاول شخص ما اختراق حسابك على فيسبوك أو سرقة كلمة السر الخاصة بك، أو حتى عندما يحاول شخص استخدام جهازك الإلكتروني بطريقة غير قانونية وكذلك النصب الالكتروني والابتزاز . كل هذه الأمور تعتبر جرائم سيبرانية

تتسم هذه الجرائم السيبرانية بالطابع الخفي والصعبة التعقب، حيث يعتمد المرتكبون على التكنولوجيا والأدوات الإلكترونية لتنفيذ هذه الأعمال الإجرامية.

لا تعترف الجرائم الإلكترونية بالحدود الجغرافية يمكن ارتكاب هذه الجرائم من أي مكان في العالم، وقد تكون الضحايا في بلد آخر تمامًا.

تتسم الجرائم الإلكترونية بصعوبة الكشف عنها بسهولة وتتبع الجناة، خاصة إذا كانوا يستخدمون تقنيات التشفير والتخفي لإخفاء هويتهم.

الجرائم الإلكترونية قادرة على التسبب في أضرار جسيمة، سواء على الأفراد أو الشركات أو حتى الحكومات.

يمكن أن تؤدي إلى فقدان الثقة في النظام المعلوماتي، والتسبب في خسائر مالية ضخمة، وحتى المساس بالأمن القومي.

الجرائم الإلكترونية مرتبطة بشكل كبير بالتكنولوجيا والتطور السريع للتقنيات الرقمية. بما في ذلك البرمجيات الخبيثة والاختراقات الأمنية.

ويمكن أن تترك آثاراً سلبية على الضحايا

تخيل للحظة!!

أنك تستيقظ في يوم مشمس جميل، لتكتشف أن معلوماتك الخاصة والحساسة غادرت مأمن حدود الخصوصية، لتنتشر في أرجاء العالم الرقمي.

مرعب أليس كذلك؟

تنبض قلوبنا بالخوف مجرد تفكيرنا في هذا السيناريو، لا داعي للهلع، لكنه الواقع الذي يمكن أن يحدث في أي لحظة، إذا لم نكن حذرين.

اذا عندما يخبرك خبير تقني أن البيانات التي تمتلكها يجب حمايتها وتهز انت راسك دون اكتراث معللا انك لست برئيس وزراء او شخصية هامة لكل هذا التحفظ فلا تستعجب ان تكون انت طرفاً وسيطاً لعملية الكترونية او وسيلة سهلة لابتزاز شخصاً ما او السيطرة علي امواله او السيطره علي حياتك انت شخصياً

الطرق والاساليب التي قد تستخدم
في اختراق هاتفك وسرقة بياناتك الشخصية

تخيل معي أن هاتفك الذكي هو قلعة تحتاج إلى حماية. الأسوار العالية، والأبراج الشامخة، والحراس المتأهبين، كل هذا معد للدفاع عن القلعة.
ولكن، هل فكرت مرة بالأعداء الذين قد يكمنون خارج الأسوار؟ الأعداء الذين يتربصون بك في الظلام، متنكرون بأقنعة الرمزية، مستعدون لاختراق حصون القلعة والاستيلاء على كل شيء داخلها؟ هؤلاء الأعداء هم الهاكرز، والقلعة هي هاتفك الذكي.

الهاكرز ليسوا مجرد مجرمين يعملون بغرض السرقة والتخريب، بل هم أيضا فنانين في استخدام واستغلال التكنولوجيا. وفي عالم الأمن السيبراني، القليل من الإبداع يمكن أن يحدث ضرراً كبيراً. فما هي الطرق التي يمكن أن يستخدمها الهاكرز لاختراق هاتفك؟ هل تعرف؟

الهاكرز ليسوا ببساطة مجرمين إلكترونيين يقومون بتنفيذ أوامر خبيثة على الأجهزة الرقمية. بل هم استراتيجيون، خبراء في فن الخداع والمناورة.
يمكنهم تشكيل هجومهم ليتناسب مع الضحية المستهدفة، مستغلين كل ما يعرفونه عن اهتمامات الضحية وما يحب.

لنأخذ لحظة لنتخيل حياة احمد علي سبيل المثال ، هو محب للموسيقى ومدون في وقت فراغه. ينشر احمد تقييمات ومقالات حول الألبومات الموسيقية الجديدة على مدونته وعلى مواقع السوشيال ميديا. يستمتع بالمشاركة في المناقشات الموسيقية وتقاسم الأفكار مع الآخرين الذين يشاركونه الشغف.

يلاحظ الهاكر النشاط الديناميكي لاحمد على الإنترنت ويرى فرصة.
يبدأ الهاكر بمتابعة احمد ، يتعرف على الفرق الموسيقية التي يحبها، الألبومات التي يترقبها، والمواقع التي يراجعها عادة.

بعد أن جمع معلومات كافية، ينشئ الهاكر رسالة بريد الكتروني مزيفه او رساله بحسابات وهمية علي موقع من مواقع التواصل الاجتماعي، تبدو كما لو كانت تأتي من موقع موسيقي يفضله احمد.

تحتوي الرسالة على خبر حصري عن الألبوم الجديد لفرقة موسيقية يحبها احمد ، مع رابط للاستماع إلى الألبوم مقدمًا. متحمس، ينقر احمد على الرابط ، لكن بدلاً من الألبوم، يحمل هاتف احمد تطبيقاً خبيثًا مصممًا خصيصًا للوصول إلى معلوماته الشخصية. بهذه الطريقة، يتمكن الهاكر من الوصول إلى هاتف احمد ويبدأ في سرقة المعلومات.

الخداع الإلكتروني (الفيشينج)

الفيشينج هو إحدى التقنيات الأكثر استخداماً بين الهاكرز لاختراق الأجهزة المحمولة. تتمثل طريقة عمل الفيشينج في استغلال الثقة بين الشخص والمؤسسة أو الشخص الذي يتصل به، حيث يقوم الهاكر بإنشاء رسالة أو صفحة ويب تبدو وكأنها من جهة موثوقة، ولكن الهدف منها في الواقع هو جمع المعلومات الحساسة مثل كلمات السر وبيانات الدخول.

الهاكرز غالبًا ما يستخدمون الرسائل علي مواقع السوشيال ميديا او علي الهاتف أو رسائل البريد الإلكتروني لتنفيذ هجمات الفيشينج.

هذه الرسائل تحتوي عادة على رابط يقود الضحية إلى صفحة ويب مزورة هذه الصفحة تكون عادة مشابهة لصفحة تسجيل الدخول لخدمة ما، مثل بنك أو منصة وسائل تواصل اجتماعي. عند إدخال الضحية لبياناتها، يتم التقاطها من قبل الهاكرز.

مثلاً تتلقى رسالة نصية تقول بأنها مثلاً من البنك الاهلي، وتحذرك من ان حسابك قد يتوقف.الرسالة تدعوك للنقر على رابط مرفق للتحقق من بياناتك وتأكيد هويتك. تبدو الرسالة مقنعة وتبدو العناوين والأرقام المرفقة فيها حقيقية.

عند النقر على الرابط، تنتقل إلى صفحة ويب تبدو تماماً مثل صفحة الدخول إلي الخدمه التي تستخدمها عادة. تقوم بإدخال اسم المستخدم وكلمة المرور الخاصة بك، ثم يطلب منك النظام إدخال بعض المعلومات الأخرى مثل رقم البطاقة المصرفية والرقم السري .

في الواقع، الرسالة النصية والصفحة التي قمت بالدخول إليها ليستا من البنك. بدلاً من ذلك، كل ما أدخلته من معلومات قد انتقل مباشرة إلى الهاكر الذي أرسل الرسالة النصية. بمعلوماتك في يده، يمكن للهاكر الآن الوصول إلى حسابك المصرفي.

التطبيقات الخبيثة

هي برامج ضارة تم تصميمها خصيصاً للقيام بأعمال غير مرغوب فيها على الأجهزة المحمولة. بمجرد تثبيتك للتطبيق والسماح بالوصول الي الاذونات، هذه الأعمال قد تشمل الوصول غير المصرح به إلى البيانات الشخصية، تتبع الموقع الجغرافي، وغيرها من الأنشطة الضارة. تأتي هذه التطبيقات غالباً متنكرة في شكل تطبيقات تبدو آمنة ومفيدة، ولكنها تحتوي على كود ضار مخفي.

يمكن للتطبيقات الخبيثة الوصول إلى وسرقة معلومات حساسة مثل جهات الاتصال، والرسائل النصية، والصور والفيديوهات، ومعلومات حساباتك في البنوك ، سجل المكالمات

وقد تقوم بتتبع موقعك الجغرافي، أو تسجيل المكالمات، أو حتى الوصول إلى كاميرا الهاتف وميكروفونه دون علمك

والبعض الآخر من التطبيقات الخبيثة قد يمنح الهاكرز القدرة على التحكم في الجهاز عن بعد، مما يتيح لهم تثبيت المزيد من البرامج الضارة او رؤية شاشة هاتفك بشكل حي

يمكن للتطبيقات الخبيثة إرسال رسائل نصية غير مرغوب فيها أو رسائل بريد إلكتروني تحتوي على روابط أو مرفقات ضارة إلى جهات اتصالك او اجراء مكالمه من هاتفك.

بعض التطبيقات الخبيثة قد تقوم بتسجيل المفاتيح التي تضغط عليها لجمع معلومات حساسة مثل كلمات السر والبيانات

هجمات من الشبكات اللاسلكية (Wi-Fi Sniffing):

عندما تقوم بتوصيل هاتفك بشبكة واي فاي مفتوحة أو غير آمنة، فأنت تضع نفسك في خطر. الهاكرز يستخدمون أدوات خاصة لرصد واعتراض البيانات التي يتم إرسالها واستقبالها عبر الشبكة.

مثال: إذا كنت تستخدم الواي فاي المفتوح في الكافيهات أو المطارات للقيام بأعمال حساسة مثل المصرفية عبر الإنترنت، فقد تكون البيانات التي تتبادلها عبر الشبكة قابلة للتجسس والاستيلاء عليها من قبل الهاكرز.

هجمات الرسائل النصية (SMS Attacks):

يستخدم الهاكرز الرسائل النصية كوسيلة لتنفيذ الهجمات. يمكن أن تكون هذه الهجمات في شكل روابط ضارة تتم إرسالها عبر الرسائل النصية، أو رسائل تحتوي على برمجيات خبيثة تتم تثبيتها عند فتح الرسالة.

مثال: قد تتلقى رسالة نصية تحتوي على رابط لتحديث تطبيق ما، ولكن النقر على الرابط يؤدي إلى تثبيت برنامج خبيث على هاتفك.

هجمات الهندسة الاجتماعية (Social Engineering):

هذه الهجمات تستند إلى استغلال الثقة البشرية. قد يتظاهر الهاكر بأنه شخص آخر – ربما صديق أو موظف في شركة تثق بها – لإقناعك بتقديم معلومات حساسة.

مثال: قد تتلقى مكالمة من شخص يدعي أنه من خدمة العملاء لشركة الاتصالات، يطلب منك تقديم كلمة المرور لحسابك لحل مشكلة فنية. إذا

قدمت المعلومات، فقد تمكنت من إعطاء الهاكر الوصول إلى حسابك.

الاستغلال عبر رمز الاستجابة السريعة (QR Code Exploitation):

مع الزيادة في استخدام أكواد الاستجابة السريعة (**QR Codes**) لتبسيط العمليات مثل الدفع والدخول إلى المواقع، يقوم بعض الهاكرز بتصميم أكواد استجابة سريعة خبيثة تربط الضحية بموقع ويب ضار أو تقوم بتحميل برنامج خبيث على الهاتف.

مثال: قد ترى كود استجابة سريعة في منشور على وسائل التواصل الاجتماعي يعدك بتخفيضات مذهلة، لكنه بمجرد مسحه، يحولك إلى موقع ويب يسرق معلوماتك الشخصية أو يقوم بتثبيت برنامج خبيث على هاتفك.

الاستغلال عبر بلوتوث (Bluetooth Exploitation):

تعتبر البلوتوث من الأدوات التكنولوجية المشهورة والمستخدمة في كل مكان، ولكنها قد تكون نقطة ضعف أمام الهاكرز. يمكن للهاكرز استغلال الثغرات في البلوتوث للوصول إلى الأجهزة والبيانات.

مثال: من خلال استخدام تقنية معروفة بـ"التنصت الأزرق" (**BlueSnarfing**)، يمكن للهاكر الحصول على الوصول إلى المعلومات الشخصية، مثل الاتصالات والرسائل النصية، وحتى الصور على هاتفك عبر البلوتوث.

الاستغلال عبر USB (USB Exploitation):

الأجهزة التي تتصل عبر منفذ **USB**، مثل الشواحن والأقراص الصلبة، يمكن أن تكون مصدراً للبرامج الخبيثة التي يمكن أن تتسلل إلى الهاتف.

مثال: توصيل هاتفك بشاحن **USB** في مكان عام، مثل محطة القطار أو المطار، قد يكون خطيراً، لأنه يمكن للشاحن أن يكون مزوداً ببرنامج

خبيث يتم تثبيته على الهاتف فور التوصيل.

الهجمات عبر الشبكات المحمولة (Cellular Network Attacks):

الهاكرز يستطيعون استغلال الثغرات الأمنية في الشبكات المحمولة لاعتراض ورصد الرسائل النصية والمكالمات. هذا يعني أن الرسائل التي تتضمن معلومات حساسة، مثل رموز التحقق المكونة من خطوتين، قد تكون عرضة للسرقة.

مثال: بعض الهاكرز يستخدمون جهاز يُعرف باسم "جهاز الاعتراض الدولي" (**IMSI Catcher**)، الذي يتظاهر بأنه برج خلوي لاعتراض الاتصالات المحمولة.

الاستغلال عبر NFC (Near Field Communication) (Exploitation):

NFC هو التقنية التي تتيح للأجهزة التواصل عبر مسافات قصيرة. يمكن أن يستغل الهاكرز ثغرات في **NFC** لنقل البرامج الخبيثة أو سرقة المعلومات.

مثال: إذا كان هاتفك مجهزًا بتقنية **NFC** وتم تمكينه، فقد يكون قادرًا على تلقي البيانات من بطاقات **NFC** خبيثة أو أجهزة أخرى، والتي قد تحمل برنامجًا خبيثًا أو تقوم بتوجيهك إلى صفحة ويب ضارة.

هل تعلم انه لا يشترط تجنب تحميل التطبيقات من مصادر غير موثوقه لاختراق هاتفك وانه يمكن لتطبيقات موجود علي متجر بلاي ويتم تنزيلها يمكنها من تسرب معلوماتك الشخصية ؟

توفر متاجر التطبيقات مثل متجر جوجل بلاي مجموعة واسعة من التطبيقات التي يمكننا تحميلها واستخدامها.

ومع ذلك، يتعين علينا أن نتذكر أن ليس كل التطبيقات موثوقة. بعض التطبيقات الخبيثة يمكن أن تكون متنكرة كتطبيقات شرعية وتطلب الإذن للوصول إلى معلوماتنا الشخصية وصورنا.

تخيل أنك حملت تطبيق تحرير الصور يعد بتحويل الصور العادية إلى أعمال فنية مذهلة. الواجهة بسيطة والمراجعات إيجابية، ولكن الشيء الذي لم تلاحظه هو أن التطبيق طلب الإذن للوصول إلى صورك وملفاتك. من غير الواضح لماذا يحتاج تطبيق تحرير الصور إلى الوصول إلى جميع ملفاتك، لكنك قد تجاهلت ذلك ووافقت على الأذونات دون تفكير.

ومع مرور الوقت، تلاحظ أن بعض الصور الشخصية التي لم تشاركها مع أحد قد ظهرت على الإنترنت، وأن بعض المعلومات الشخصية لديك قد تم تسريبها. وهكذا، من خلال التطبيق الذي ظننت أنه سيحول صورك إلى تحف فنية

وعلي النقيض

دعونا نتخيل سيناريو. تبحث عن تطبيق لتحرير الصور يمكنه تحويل صورك العادية إلى أعمال فنية. تجد تطبيقًا يعد بذلك ويبدو جذابًا وموثوقًا ومن الطبيعي أن يطلب تطبيق تحرير الصور هذا الوصول إلى معرض صورك. وبدون أي تردد، تقدم بإعطاء هذا التطبيق الوصول إلى صورك.

لكن ماذا لو كان خلف الواجهة الجذابة للتطبيق شخصٌ بنياته ليست جيدة؟ ماذا لو كان الهدف الحقيقي لهذا التطبيق هو جمع صورك وإرسالها إلى متسللين؟ هذا السيناريو ليس خياليًا، بل حقيقة موجودة تحدث في عالم الإنترنت.

تطبيق "تحفة الفن"، كما سنسميه، يحتاج بالفعل إلى الوصول إلى صورك لتتمكن من تحريرها. لكنه في الواقع يستغل هذا الإذن للوصول إلى جميع صورك وإرسالها إلى خارج الهاتف دون علمك. هذا النوع من الاختراقات الذكية يمكن أن يكون صعب الكشف حتى لأكثر الأشخاص وعيًا بالأمان الإلكتروني حتي لن يظهر أي تنبيه من اي فاحص فيروسات او حتي متجر جوجل بأن هذا التطبيق يقوم بسرقة بياناتك.

"عندما يتحول الخفاء إلى واقع مرعب، وتصبح أدواتنا اليومية مسرحًا للجريمة الرقمية. بين أطياف الرموز والأكواد، ينتظر خطر غامض، يمتص الخصوصية ويبتلع الأمان. هل أنت مستعد لاستكشاف المزيد، حيث الأصدقاء يتحولون إلى أعداء والأمانات تصبح خيانات؟
الآن أعد النظر في هاتفك، هل ما زال يشعرك بالأمان؟
هل أصبح الشكوك تساورك؟

الآن هو الوقت للكشف عن الحقائق المرعبة التي تقبع خلف شاشة هاتفك..."

الطرق والاساليب التي قد تستخدم
في اختراق حساباتك علي مواقع التواصل الاجتماعي

تجتاح رياح الإثارة والغموض، ونحن على أعتاب رحلة في عالم القراصنة الإلكترونيين، أولئك الذين يسرقون الهويات ويشوهون الحقائق. في هذا العالم، تُدار معارك الأمان والخصوصية بعيداً عن الأعين، وراء الشاشات. إحدى أكثر الطرق شيوعًا وفعالية التي يستخدمها القراصنة هي "الصيد الاحتيالي" أو **Phishing**، حيث يتظاهرون بأنهم جهة موثوقة لتحصيل معلوماتك الشخصية. على سبيل المثال، قد تتلقى رسالة بريد إلكتروني تبدو وكأنها من فريق دعم فيسبوك، تطلب منك تحديث بياناتك الشخصية لتأكيد هويتك. بمجرد النقر على الرابط المرفق، تجد نفسك على صفحة تسجيل الدخول التي تبدو مشابهة تمامًا لفيسبوك. ولكنها في الواقع صفحة مزيفة تم إنشاؤها لجمع بيانات الدخول الخاصة بك .

تقنية أخرى مشهورة هي "الهجوم الوسيط" أو **Man in the Middle**، حيث يقف الهاكر بينك وبين الشبكة التي تتصل بها لاعتراض بياناتك.

على سبيل المثال، قد تستخدم شبكة **Wi-Fi** عامة في مقهى لتحديث حالتك على **Instagram**. ولكن الشبكة التي تستخدمها قد تكون تحت سيطرة هاكر يستطيع رؤية كل ما ترسله وتستقبله.

الهجمات القاموسية أو **Brute Force Attacks**: في هذه الطريقة، يستخدم الهاكر برنامجًا يجرب تسلسلات متعددة وعشوائية من الأحرف والأرقام حتى يتمكن من تخمين كلمة المرور الخاصة بك. إذا كانت كلمة المرور الخاصة بك ضعيفة أو شائعة، فقد يكون من السهل على الهاكر اختراق حسابك.

الهجمات الاجتماعية أو **Social Engineering**: هذا يتضمن استخدام المعلومات الشخصية للاختراق. قد يحاول الهاكر التواصل معك شخصيًا، أو من خلال الأشخاص الذين تثق بهم، للحصول على معلومات يمكن استخدامها لاستعادة كلمة المرور أو الدخول إلى حسابك.

مالوير أو **Malware**: هي البرمجيات الخبيثة التي يمكن تثبيتها على جهازك بدون علمك عند تنزيل تطبيق غير آمن أو فتح رابط غير موثوق. البرمجيات الخبيثة هذه يمكن أن تسجل مفاتيح الضغط وتراقب الأنشطة على جهازك وتسرق بيانات الدخول الخاصة بك.

الطرق والأساليب التي يمكن استخدامها لإخفاء محادثات الواتساب، واسترجاع المحادثات حتى وإن تم حذفها

1-اخفاء المحادثات في النسخ المعدلة

التواصل في العالم الرقمي الحديث أصبح أكثر من مجرد تبادل للرسائل، فهو بمثابة القلم الذي نرسم به لوحات حياتنا اليومية. واتساب، هذاالتطبيق المعروف، هو الأداة التي نستخدمها في كل يوم، ولكن

هل تعلم أن هناك نسخاً معدلة من واتساب تتيح لك فن إخفاء المحادثات وراء اسم الواتساب؟

بصفتك زوجة ترغب في الحفاظ على بعض المحادثات بعيداً عن الأنظار، أو أخت تود حفظ بعض الأسرار مع أصدقائها، أو حتى كزوج يتطلع إلى إبقاء بعض الأمور خاصة، اغلب النسخ المعدله من واتساب تقوم بذلك.

كل ما عليك فعله هو الضغط مرتين على اسم واتساب، وكأنك تستخدم سحر خفاء لتجعل المحادثات تختفي أو تظهر حسب رغبتك مثلما يكشف الساحر عن الأرنب من قبعته، مع كل ضغطة يتغير العالم خلف الشاشة، حيث يتم إخفاء المحادثات أو إظهارها بكل سلاسة ويسر.

ربما يكون هذا الأمر بمثابة فتح باب إلى عالم آخر، عالم مليء بالأسرار والكشف عنها. فمن خلال هذه الخاصية، يمكنك التحكم في المعلومات التي تظهر والتي تختفي. يمكن أن يكون هذا عالمًا مثيرًا وجديدًا، مليء بالأسرار والألغاز التي تنتظر الكشف عنها.

خدعه في اخفاء المحادثات

لكل سر جانب غامض ومثير للاهتمام قد تظن أنك فتحت باب المحادثات المخفية بالضغط مرتين على اسم "واتساب"، لكن هنا تأتي اللعبة الحقيقية.

فقد يتم تعطيل هذه الخاصية في بعض الأحيان، حيث تصبح المحادثات المخفية غير قابلة للظهور مرة أخرى حتى بعد الضغط المتكرر على الاسم.

مثلا، تخيل أنك في غرفة مظلمة وأنت تبحث عن مفتاح النور، تعتقد أنه فقط بالضغط على الزر، ستنير الغرفة. لكنك تكتشف أن الزر لا يعمل، وعليك أولاً البحث عن القاطع الكهربائي لتعيد تشغيله.

هكذا يحدث ، حيث انه يمكن تعطيل خاصية الضغط على اسم واتساب لإظهار المحادثات المخفية. فتضغط مرتين، ثلاث، أو حتى عشر مرات، ولن تظهر لك المحادثات المخفية .

السر هنا في الاعدادات، حيث يجب عليك أولاً تفعيل هذه الخاصية لتتمكن من الوصول إلى المحادثات المخفية.

ومع ذلك، فإن السرية والخصوصية المفرطة قد تتحول إلى سلاح ذو حدين. قد تظن أنك تحافظ على الأسرار المدفونة عميقاً، ولكن في الواقع، قد تكون تخلق الجو الكامل للشك والتوتر.

قد يصبح الشريك أو الأصدقاء أو الأسرة على حذر، وربما يشكون في وجود شيء غير صحيح. إذا تم اكتشاف هذه الميزة من قبل الآخرين، سيكون الأمر بمثابة تحول جذري، والشخص الذي كنت تعتقد أنه سيكون ملاذك الآمن، يمكن أن يتحول إلى مصدر القلق.

الأداة التي كنت تعتبرها درعًا قويًا لحماية الأسرار، قد تتحول إلى سيف يهدد بالكشف عن كل شيء. في النهاية، ما خفي كان أعظم.
لذا، عند استخدام هذه الميزة، يجب التفكير في العواقب المحتملة. هل هي فعلاً ضرورية؟ هل يمكنك التعامل مع النتائج إذا تم الكشف عن المحادثات المخفية؟ هل يمكن أن يكون الأمر ضاراً أكثر من الفائدة؟ الأسئلة متعددة، ولكن القرار في النهاية يعود لك.
من الأفضل دائمًا الصراحة والشفافية وفي حالة الشكوك، يجب دائمًا تذكر أن الثقة مرة واحدة فقط، إذا ضاعت، فإنها تحتاج إلى الكثير من الوقت والجهد لتعود مرة أخرى.

2-ميزة قفل الدردشة

هل سبق أن تمنيت أن تضع محادثاتك في خزانة مغلقة بمفتاح؟
هل أردت أن تعيش حياة خالية من القلق بشأن سرقة معلوماتك الخاصة وتسربها؟ قد تكون هذه الرغبات قد تحققت بالفعل ، أعلنت **Meta** عن طبقة أمان جديدة تقدمها للمستخدمين عبر تطبيق **WhatsApp**.
تحمل الميزة الجديدة اسم "قفل الدردشة"، وتأتي لتقدم لك طريقة آمنة ومبتكرة للحفاظ على سرية محادثاتك.
تتيح لك هذه الميزة نقل المحادثات إلى مجلد خاص يشبه خزانة الأمان، حيث يمكنك الاحتفاظ بمحادثاتك الهامة بعيداً عن العيون الفضولية.
لنتخيل سويا، أنت في مقهى مزدحم وتتلقى رسالة ذات أهمية خاصة. تتوجه نظر الجميع نحو هاتفك، ولكن بفضل "قفل الدردشة"، لن يظهر اسم المرسل ولا محتوى الرسالة.

حتى أن ملفات الوسائط المرفقة لن تظهر في معرض الهاتف، فكل شيء يبقى خاصاً وآمناً في هذا الخزانة الرقمية.

مع إمكانية إنشاء كلمة مرور مخصصة لفتح الدردشات المقفلة. تخيل أن لديك مفتاح خاص لكل دردشة، مفتاح يفتح عالم الأسرار والمحادثات الخاصة.

الذكاء الاصطناعي الحرب الباردة

في أروقة المدينة، وتحت ظلال الأسرار التي تحتضنها الليالي، ظهرت تكنولوجيا قد تغير الحقائق كلها.

لو كنت تعتقد أن أذنيك هي أفضل شهيد، فقد تحتاج للتفكير مرة أخرى.

هل سمعت عن تلك التسجيلات الصوتية المتلاعبة التي بدأت تنتشر كالنار في الهشيم؟ قد تأتيك رسالة من صديق قديم، أو من حبيبك، أو حتى من والدك، وتظن أنها حقيقية! لكن الحقيقة، هي أن هذه الأصوات مُحتمل أن تكون مُلفقة.

بفضل أدوات الذكاء الاصطناعي المتطورة، أصبح بإمكان الجميع – حتى الأطفال – أن يُحاكوا أصواتًا مألوفة بدقة عالية. تخيل أن تستيقظ ذات يوم لتسمع تسجيلًا يقول فيه أحدهم بصوتك: "أنا مُذنب" أو "أنا أحبك" لشخص لم تقل له هذا من قبل!

وفي ممرات الظلام وأروقة الغموض، قد يحاول البعض استغلال هذه التكنولوجيا في أمور قد تسبب الكثير من المشاكل. تسجيلات مُلفقة قد تُهدد حياتك، أو مستقبلك، أو حتى علاقاتك.

لذلك، قبل أن تأخذ قرارًا بناءً على أي تسجيل صوتي تسمعه، تأكد من مصداقيته. فالذكاء الاصطناعي أصبح لا يميز بين الحقيقة والخيال، ولكن القلب والعقل ما زالا يملكان القدرة على فرز الحقائق..

وفي هذه اللحظة، يظهر السؤال الأكبر: إلى أين نحن ذاهبون بهذه التكنولوجيا الفاتنة ولكنها خطيرة؟

بمرور الوقت، وبزيادة الاهتمام بأدوات الذكاء الاصطناعي، نجد أن دائرة المستخدمين تتسع يومًا بعد يوم. الجميع، من المحترفين وصولًا إلى الهواة، أصبح لديهم القدرة على التلاعب بالأصوات وصنع الواقع الافتراضي الخاص بهم.

ومع هذه الانتشار الواسع، أصبحت هذه الأدوات أكثر دقة، وأكثر خطورة. مثلما يتطور الطب، وتظهر أدوية جديدة للأمراض التي كانت مستعصية في الماضي، هكذا أيضًا تتطور أدوات الذكاء الاصطناعي لتكون أكثر احترافية. لكن السؤال هو: هل نحن مستعدين للتعامل مع هذه القوة الهائلة؟

فمع كل انتشار، يتضاعف عدد الضحايا. أناس بريئون قد يتعرضون للأذى بسبب تسجيل صوتي ملفق. الأمور الخاصة قد تُفضح، والأكاذيب قد تُروج، والحقائق قد تُعتبر أوهامًا

ففي عالم حيث الواقع والخيال يصبحان وجهي نقطة واحدة، يصبح علينا جميعًا أن نكون أكثر حذرًا ويقظة. نحن بحاجة إلى استعادة قوتنا في التمييز بين الحقيقة والوهم، وأن نتذكر دائمًا أن الأذن قد تخدع، ولكن القلب يعرف الطريق إلى الحقيقة